UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

9

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,770	05/11/2001	Satoshi Shigematsu	96790P355	6640

8791 7590 06/11/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
06/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/853,770	**Applicant(s)** SHIGEMATSU ET AL.
	Examiner Ellen C. Tran	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-36 and 51-99* is/are pending in the application.

4a) Of the above claim(s) *51-82 and 94-99* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-36 and 83-93* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)☒ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/853,770.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 13 Nov '06

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 27 March 2007 with an original application filed 11 May 2001, with acknowledgement of foreign priority date 12 January 2001.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 27 March 2007 has been entered.

3. Claims 1-2, 4-36, and 83-99 are currently pending in the application. Claims 1, 10, 21, 25, 29, 33, 94, 95, 96, 97, 98, and 99 are independent claims. Claims 51-82 are withdrawn. Claims 3 and 37-50 have been canceled. Claims 1, 10, 21, 25, 29, 33-36, 83-93 are amended, claims 94-99 are new, amendments to the claims are accepted.

Information Disclosure Statement

4. The IDS submitted 13 November 2006 has been considered.

Claim Objections

5. Claims 94-99 are objected to because of the following informalities: The claims all use the notation "/" which could be interpreted as "and or" which is an indefinite phrase . Appropriate correction is required.

Response to Arguments

6. Applicant's arguments with respect to claims 1-2, 4-36, and 83-99 filed 27 March 2007 have been fully considered but they are moot due to new grounds of rejection below initiated by amendment to all the independent claims.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1-2, 4-7, 8, 20, 83-86,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. U.S. Patent No. 6,484,260 (hereinafter '260) in view of Hsu et al. U.S. Patent No. 6,041,410 (hereinafter '410).

As to independent claim 1, "An authentication token which is normally held by a user and, when the user is to use a device for executing predetermined processing in accordance with authentication data of the user, connected to the device to perform user authentication on the basis of biometrical information of the user, comprising: a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result as authentication data representing a user

authentication result; a communication unit for transmitting the authentication data from said personal collation unit to the device as communication data, wherein said personal collation unit and communication unit are integrated" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"and a protocol conversion unit for converting format of the communication data to be transmitted to the device into a format that can be received and decoded by the device that can be received and decoded by the device wherein said personal collation unit and communication unit are integrated" however '410 teaches that after the correlation unit verifies the sensed biometrics the portable device transmits an encrypted numerical data wherein the door provides the desired access in col. 2, lines 36-57.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '410. One in the art would have been motivated to perform such a modification because as indicated by '410 there is a widely felt need for a more reliable technique for limiting access (see '410 col. 1, lines 42 et seq.) "Accordingly, there is a widely felt need for a more reliable technique for limiting access to personal property and other valuable assets. Ideally, the technique should positively verify the identity of the person seeking access, and should eliminate the need to carry multiple keys and scannable cards, and the need to memorize combinations, passwords and PINs. The present invention satisfies this need".

As to dependent claim 2, "wherein said storage unit further stores in advance user information unique to the user, which is to be used for processing in the device, and said collation unit outputs the authentication data containing the user information read out from said storage unit" is shown in '260 col. 2, lines 15-43.

As to dependent claim 4., "further comprising a radio unit for transmitting the communication data from said communication unit to the device through a radio section" is taught in '260 col. 7, lines 35-58.

As to dependent claim 5, " further comprising a radio unit for transmitting the communication data from said protocol conversion unit to the device through a radio section" is shown in '260 col. 7, lines 35-38.

As to dependent claim 6, "further comprising a battery for supplying power" is disclosed in '260 col. 6, lines 29-39.

As to dependent claim 7, "wherein said battery comprises a secondary battery charged by power supply from the device when said authentication token is connected to the device" '260 teaches "Referring now to FIGS. 4A-4D, one embodiment of a PID 6B, which includes all the features also shown in FIG. 1, includes a housing 44 similar in size to a personal pager or a small cellular telephone" in col. 8, lines 14-40 it is obvious that a PID which is similar to a cellular phone would include rechargeable batteries.

As to dependent claim 8, "wherein said storage unit has, in addition to a storage area for storing the registered data, at least one storage area for storing another information" is taught in '260 col. 2, lines 27-38.

As to dependent claim 20, "wherein said authentication token further comprises another storage circuit for storing a password of said authentication token and token identification information for identifying said authentication token, and when the personal collation result indicates that the collation is successful, said communication unit transmits the password and token identification information in said another storage circuit to said service providing apparatus as the communication data" is taught in '260 col. 3, lines 49-63.

As to dependent claim 83, "wherein said token further comprises an encryption circuit for encrypting data generated from the authentication data and dynamic information generated by the device and transmitted using a key registered in advance, and said communication circuit transmits to the device encrypted data generated by said encryption circuit" is shown in '260 col. 2, lines 22-39;

"wherein the dynamic information changes each time it is generated" is disclosed in '260 col. 5, lines 49-58, because the random number changes with time.

As to dependent claim 84, "wherein said token further comprises a result determination circuit for, when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit, and an encryption circuit for, in accordance with the authentication data from said result determination circuit, encrypting dynamic information transmitted from the device using a key registered in advance, adding obtained encrypted data to the authentication data, and outputting the encrypted data, and said communication circuit transmits to the device the authentication data with the

encrypted data from said encryption circuit or the authentication data from said result determination circuit" is disclosed in '260 col. 2, lines 22-39.

As to dependent claim 85, "wherein said token further comprises an encryption circuit for encrypting dynamic information transmitted from the device using a key registered in advance and outputting obtained encrypted data to said first communication circuit as data, and a first result determination circuit for, when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data" is taught in '260 col. 2, lines 53 through col. 3, line 3;

"and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data that would be produced if the authentication was successful to said first communication circuit and said first communication circuit transmits to the device the data from said encryption circuit or the data from said first result determination circuit" is shown in '260 col. 3, lines 29-65 (note, Scott teaches if the authentication fails the process ends, this inherently means that the number of digits would be different).

As to dependent claim 86, "wherein said token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance, and said first communication circuit transmits to the device the identification information stored in said ID storage circuit" is disclosed in '260 col. 3, lines 23-28.

9. **Claims 9-19, 21-36, and 87-93,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. U.S. Patent No. 6,484,260 (hereinafter '260) in view of Hsu et al.

U.S. Patent No. 6,041,410 (hereinafter '410) in further view of Sumino U.S. Patent No. 6,957,338 (hereinafter '338).

As to independent claim 10, "An authentication system for executing user authentication, which is necessary for use of a device for executing predetermined processing, by using biometrical information of a user, comprising: an authentication token which is normally held by the user and, when the user is to use said device, the authentication token connected to said device and to perform user authentication on the basis of the biometrical information of the user, said authentication token comprising a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result representing a user authentication result as authentication data, a first communication unit for transmitting the authentication data from said personal collation unit to said device as communication data, and" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"and a protocol conversion unit for converting format of the communication data to be transmitted to the device into a format that can be received and decoded by the device said personal collation unit and said first communication unit being integrated" however '410 teaches that after the correlation unit verifies the sensed biometrics the portable device transmits an encrypted numerical data wherein the door provides the desired access in col. 2, lines 36-57;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '410. One in the art would have been motivated to perform such a modification because as indicated by '410 there is a widely felt need for a more reliable technique for limiting access (see '410 col. 1, lines 42 et seq.) "Accordingly, there is a widely felt need for a more reliable technique for limiting access to personal property and other valuable assets. Ideally, the technique should positively verify the identity of the person seeking access, and should eliminate the need to carry multiple keys and scannable cards, and the need to memorize combinations, passwords and PINs. The present invention satisfies this need".

the following is not taught in the combination of '260 and '410: **"and said device comprising a second communication unit for receiving the communication data transmitted from said authentication token and outputting the data as the authentication data, and a processing unit for executing the predetermined processing on the basis of the collation result contained in the authentication data from said second communication unit"** however '338 teaches "a collating unit for respectively collating the biological information and the password output" in col. 1, lines 63-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 and '410 a portable personal identification system utilizing biometrics to include a means to store passwords in the personal devices as taught in '338. One in the art would have been motivated to perform such a modification because as indicated by '338 a need exist to combine the authentication cards used that store passwords with biometrics to insure security (see '338 col. 1, lines 32-51 "However, even in the individual authentication system using the IC card, if both the IC card (a physical object) and the password (individual knowledge) are stolen, the safety is not secured ... an object of the present invention is to provide an individual authentication system by which the data processing device which needs individual authentication can be used and managed with higher security".

As to dependent claim 12, "wherein said storage unit of said authentication token stores in advance user information unique to the user, which is to be used for processing in said device, said collation unit of said authentication token outputs the authentication data containing the user information read out from said storage unit, and said processing unit of said device executes processing using the user information contained in the authentication data from said second communication unit" is taught in '338 col. 1, lines 54-67. The motivation to combine '260 and '338 is the same as stated above in claim 10.

As to dependent claim 9, "wherein said at least one storage area for storing another information includes a storage area for storing personal information of the user and a storage area for storing service information" is shown in '338 col. 1, lines 54-67. The motivation to combine '260 and '338 is the same as stated above in claim 10.

As to dependent claims 11, 13-19, and 87-93,these claims contain substantially similar subject matter as claims 3- 9 and 83-86 above; therefore they are rejected along similar rationale.

As to independent claim 25, "An authentication method of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and provides the service to the user on the basis of a collation result and an authentication token for

executing the user authentication using biometrical information of the user, wherein" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"converts formats of communication data containing the password and token identification into a format that can be received and decoded by the service proving apparatus and transmit the communication data to the service proving apparatus" however '410 teaches that after the correlation unit verifies the sensed biometrics the portable device transmits an encrypted numerical data wherein the door provides the desired access in col. 2, lines 36-57;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '410. One in the art would have been motivated to perform such a modification because as indicated by '410 there is a widely felt need for a more reliable technique for limiting access (see '410 col. 1, lines 42 et seq.) "Accordingly, there is a widely felt need for a more reliable technique for limiting access to personal property and other valuable assets. Ideally, the technique should positively verify the identity of the person seeking access, and should eliminate the need to carry multiple keys and scannable cards, and the need to memorize combinations, passwords and PINs. The present invention satisfies this need".

the following is not taught in '260 and '410:

"the authentication token stores in advance a password of the authentication token and token identification information for identifying the authentication token, performs collation on the basis of the biometrical information detected from the user to check whether

the user is an authentic user and when a collation result indicates that collation is successful" and **"and authentication token in advance in a first database in association with each other, collates the password contained in the communication data received from the authentication token with a password obtained from the first database using the token identification information as a key"** however '338 teaches "an individual authentication card for storing biological information and a password for identifying a registered user" (registered is interpreted to mean the information was provided in advance) in col. 1, lines 54-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 and '410 a portable personal identification system utilizing biometrics to include a means to store passwords in the personal devices as taught in '338. One in the art would have been motivated to perform such a modification because as indicated by '338 a need exist to combine the authentication cards used that store passwords with biometrics to insure security (see '338 col. 1, lines 32-51 "However, even in the individual authentication system using the IC card, if both the IC card (a physical object) and the password (individual knowledge) are stolen, the safety is not secured ... an object of the present invention is to provide an individual authentication system by which the data processing device which needs individual authentication can be used and managed with higher security".

As to dependent claim 26, "wherein the token identification information and password are registered in the first database in association with each other from a registration apparatus connected to the service providing apparatus through a communication network" is disclosed in '260 col. 5, lines 55-58 "The personal identification device can be used in conjunction with conventional telephone lines or computer network communications".

As to dependent claim 27, "wherein the service providing apparatus causes a password generation circuit to generate a new password, transmits the new password to the authentication token through the second communication unit, and updates the password stored in the first database, and the authentication token updates the password stored in advance by the new password received from the service providing apparatus" is taught in '260 col. 3, lines 29-67 (note the generated random number is interpreted to have the same meaning as the new password).

As to dependent claim 28, "wherein the service providing apparatus stores device identification information for identifying the service providing apparatus in advance, and transmits the device identification information to the authentication token when the authentication token is connected, and the authentication token stores in advance the password and the device identification information for identifying the service providing apparatus in a second database in association with each other, and uses, as the password to be transmitted to the service providing apparatus, a password obtained from the second database using the device identification information received from the service providing apparatus as a key" is shown in '260 col. 3, lines 29-67.

As to independent claim 29, this claim is directed to a recording medium for causing a computer to execute the authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 30-32, these claims contain substantially similar subject matter as claims 26-28; therefore they are rejected along similar rationale.

As to independent claim 33, this claim is directed to a program for causing a computer to execute the authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 34-36, these claims contain substantially similar subject matter as claims 26-28; therefore they are rejected along similar rationale.

As to independent claim 21, this claim contains the limitations previously presented in claims 1, 10, and 25; therefore it is rejected along similar rationale.

As to dependent claims 22-24, these claims contain substantially similar limitations as dependent claims 11, 27, and 28; therefore they are rejected along similar rationale.

10. **Claims 94-99,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito et al. U.S. Patent No. 6,980,672 (hereinafter '672) in view of Scott et al. U.S. Patent No. 6,484,260 (hereinafter '260).

As to independent claims 94, "A biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising: drive means for locking/unlocking the door storage means for storing the biometrical information of the user, said storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token; and processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the

biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, said processing means comprises lock means for, when the fingerprint authentication token is inserted into the main body in storing the article in the main body, controlling said drive means to lock the door" is taught in '672 col. 2, lines 1-11;

the following is not explicitly taught in '672:

"generating a new password whenever the door is locked, storing the password in said storage means, transmitting the password to the fingerprint authentication token, and causing the fingerprint authentication token to store the password, and unlock means for controlling said drive means to unlock the door when a password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in said storage means, wherein the fingerprint authentication token is independent of the main body and physically separated from the main body" however '260 teaches "Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons" (note the "password" is interpreted to have the same meaning as the "random number") in col. 3, lines 29-65.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '672 a biometrical authentication method to include a means to exchange passwords as taught in '260. One in the art would have been motivated to perform such a modification because a method is needed to combine access codes used in the past with biometric identification as indicated by '260 in order to protect the biometric information and scol. 1, lines 17-43 "Each of these security systems can be operated by any person who is in possession of the fixed code ... Therefore, each of these systems is inherently insecure ... it there is a match, the requesting person is allowed entry or access to the host facility ... However, if the set of authorized person is large, such a system would require a huge database to store the fingerprint images ... and the identification process would become slower".

As to independent claim 95, this claim contain substantially similar subject matter as claim 94, with the addition of the following limitation which are also taught by '260 and '672:

"a plurality of storage section capable of independently storing articles and having corresponding doors" however '260 teaches a plurality of door and various user access rights in col. 4, lines 61-67;

"display means for designating one of the plurality of doors, and display means for displaying a number of the door" '672 teaches the in col. 2, lines 2-3 that the lock equipment has a mechanism to lock or unlock the object that is secured; '672 teaches in col. 10, lines 12-29 how the invention can be used on a trunk allowing the authorized person to lock and un-lock the trunk by the correct placement of their authorized fingerprint; 672 teaches in col. 11, line 63 through col. 12, line 13 how the system has an LED for displaying messages in combination with the logic received from the locking mechanism and biometric inputs, it would be obvious to incorporate the ability for an LED to display a room number. This feature is similar to the other example provided where a user can determine which locker they utilized in the coin operated locker by using their fingerprint and watch the for a flashing LED see col. 18, lines 17-23.

As to independent claims 96, **"A lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising: a first step of unlocking the door on the basis of matching between stored information in storage means in advance and detected information from a sensor for detecting the biometrical information of the user, the storage means stores a fingerprint image of the user as the biometrical information, each user has a fingerprint authentication token; and processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, processing the second step comprises"** is taught in '672 col. 2, lines 1-11;

the following is not explicitly taught in '672:

"a third step of, when the fingerprint authentication token is inserted into the main body in storing the article in the main body, locking the door, generating a new password whenever the door is locked, storing the password in the storage means, transmitting the password to the fingerprint authentication token, and causing the fingerprint authentication token to store the password, and a fourth step of unlocking the door when a

password based on matching between a registered fingerprint image and the fingerprint image detected by the sensor and output from the fingerprint authentication token is received in taking out the article stored in the main body, and the received password matches the password in said storage means, wherein the fingerprint authentication token is independent of the main body and physically separated from the main body" however '260 teaches "Other steps include generating, at the host facility, a random number signal representing a random number in response to the ID code signal only if the ID code signal is representative of the ID code of the device controlled by one of the registered persons" (note the "password" is interpreted to have the same meaning as the "random number") in col. 3, lines 29-65.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '672 a biometrical authentication method to include a means to exchange passwords as taught in '260. One in the art would have been motivated to perform such a modification because a method is needed to combine access codes used in the past with biometric identification as indicated by '260 in order to protect the biometric information and scol. 1, lines 17-43 "Each of these security systems can be operated by any person who is in possession of the fixed code ... Therefore, each of these systems is inherently insecure ... it there is a match, the requesting person is allowed entry or access to the host facility ... However, if the set of authorized person is large, such a system would require a huge database to store the fingerprint images ... and the identification process would become slower".

As to independent claim 97, this claim is substantially similar to independent claim 96 with the addition of the following limitation that are also taught in the prior art references.

"a plurality of storage section capable of independently storing articles and having corresponding doors" however '260 teaches a plurality of door and various user access rights in col. 4, lines 61-67;

"display means for designating one of the plurality of doors, and display means for displaying a number of the door" '672 teaches the in col. 2, lines 2-3 that the lock equipment has a mechanism to lock or unlock the object that is secured; '672 teaches in col. 10, lines 12-29 how the invention can be used on a trunk allowing the authorized person to lock and un-lock the trunk by the correct placement of their authorized fingerprint; 672 teaches in col. 11, line 63 through col. 12, line 13 how the system has an LED for displaying messages in combination with the logic received from the locking mechanism and biometric inputs, it would be obvious to incorporate the ability for an LED to display a room number. This feature is similar to the other example provided where a user can determine which locker they utilized in the coin operated locker by using their fingerprint and watch the for a flashing LED see col. 18, lines 17-23.

As to independent claims 98 and 99, these claims contain substantially similar subject matter as claims 94-97 above and therefore they are rejected along similar rationale.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen

Ellen Tran
Patent Examiner
Technology Center 2134
4 June 2007